



Date de réception : 23/01/2015

CURIA GREFFE
Luxembourg
Entrée 14 NOV. 2014

WE HEREBY CERTIFY THE
WITHIN TO BE A TRUE
COPY OF THE ORIGINAL

TO THE PRESIDENT AND MEMBERS
OF THE COURT OF JUSTICE
OF THE EUROPEAN UNION

11 11 23
GERARD RUDDEN
SOLICITOR
5 CLARE ST.
DUBLIN 2

IN CASE C-362/14

MAXIMILLIAN SCHREMS

Applicant

V.

DATA PROTECTION COMMISSIONER

Respondent

AND

DIGITAL RIGHTS IRELAND LIMITED

Amicus curiae

WRITTEN OBSERVATIONS OF APPLICANT

Maximillian Schrems, pursuant to the second paragraph of Article 23 of the Protocol on the Statute of the Court of Justice, represented by Mr. Noel J. Travers, Senior Counsel, and Mr. Paul O'Shea, Barrister, both of the Bar of Ireland, as well as by Professor Herwig Hofmann, Rechtsanwalt, of the Cologne Bar, Germany, all instructed by Mr. Gerard Rudden, Solicitor, of Ahern Rudden Solicitors, 5 Clare Street, Dublin 2, Ireland, has the honour of submitting the following written observations to the Court of Justice of the European Union on the questions referred for preliminary ruling pursuant to Article 267 TFEU by the High Court of Ireland, by orders of that Honourable Court of 16th and 25th July 2014, received at the Registry of the Court of Justice of the European Union on 26th August 2014.

Registered at the
Court of Justice under No. 378006
Luxembourg, 17. 11. 2014
Fax/E-mail: 11.11.14 For the Registrar
Received on: 14.11.14 Lynn Hewlett
Principal Administrator

TABLE OF CONTENTS¹

I.	INTRODUCTION AND OVERVIEW	2
II.	LEGAL AND FACTUAL BACKGROUND	3
A.	Factual context and order of reference of High Court	3
B.	Core applicable EU law provisions.....	7
(i)	<i>Right to privacy, data protection, an effective remedy and to a fair trial</i>	7
(ii)	<i>Directive 95/46</i>	8
(iii)	<i>Commission Decision 2000/520/EC of 26 July 2000 ("the SHD")</i>	9
C.	Questions referred & provisional view of High Court	10
III.	ANALYSIS	11
A.	Overview	11
B.	Invalidation of the SHD.....	13
(i)	<i>Incompatibility of the SHD with Article 25 of the Directive 95/46</i>	13
(ii)	<i>Incompatibility of the SHD with fundamental rights protection in EU law</i>	15
a)	<i>Right to privacy under Directive 95/46</i>	15
b)	<i>Scope of right to privacy with regard to processing of personal data in EU law</i>	16
c)	<i>Limitation of rights guaranteed by Articles 7 and 8 CFR</i>	19
d)	<i>Proportionality</i>	20
(iii)	<i>Invalidity of the SHD for failure to ensure for control by an independent authority</i>	25
(iv)	<i>Invalidity of the SHD due to incompatibility with the right to an effective remedy in EU law</i>	27
C.	Obligation of the DPC to take appropriate action	30
IV.	CONCLUSION	31
	LIST OF ANNEXES	33

I. INTRODUCTION AND OVERVIEW

1. This preliminary reference has arisen from judicial review proceedings before the High Court of Ireland, wherein Maximillian Schrems, the applicant, challenges the legality of a decision by the Irish Data Protection Commissioner ("DPC"), the respondent, not to investigate a complaint lodged on 25th June 2013. Subsequent to letters dated 25th and 26th July 2013, the DPC invoked powers under the Irish Data Protection Act 1988 ("the 1998 Act") not to investigate Mr. Schrems' complaint on the ground that it was legally unsustainable.² This conclusion was based the DPC's

¹ The following abbreviations will, in the interest of brevity, be used in these written observations (amongst others that are defined in the text):

CFR = Charter of Fundamental Rights of the European Union;

ECHR = European Convention on Human Rights;

ECtHR = European Court of Human Rights;

US/USA = United States/ United States of America.

² Formally, the DPC found that the complaint was "*frivolous and vexatious*", but, as a matter of Irish data protection law, as confirmed by the referring court, this simply has the technical meaning that the complaint could not succeed. The *bona fides* of the applicant and the genuineness of his complaint was not disputed by the DPC and, moreover, has been fully upheld by the High Court in its judgment of 18th June 2014 ("the judgment of 18 June 2014"), at para. 16, which judgment underlies the order for reference and is at Appendix 2 thereto.

view that he was 'bound' by Commission Decision 2000/520/EC of 26 July 2000 ("SHD").³ The correctness of this view, as a matter of EU law, is central to this preliminary reference. In the SHD the Commission concluded over 14 years ago that, what are set out in Annex I thereto and described therein as the 'Safe Harbor Privacy Principles' ("SHPs"), provide adequate protection, with regard to the personal data transferred from the EU/EEA to the United States. The personal data of the applicant are transferred to the USA by Facebook Ireland Ltd ("Facebook Ireland").⁴

2. If the Commission's July 2000 conclusion in the SHD as to the adequacy of protection of personal data transferred to the USA is no longer binding on national data protection authorities ("DPAs"), like the DPC in the main proceedings, the High Court has expressed the firm view that the applicant would be entitled, under the fundamental right to privacy protected under Irish constitutional law, to succeed in his judicial review application. Thus, central to this case is whether, as a matter of EU law, the Commission's adequacy assessment in the SHD binds DPAs, notwithstanding the dramatically changed factual circumstances that have been found to exist by the High Court; *i.e.*, the "*mass and undifferentiated*" access that is available to the US National Security Authority ("NSA") and other US security agencies to the personal data that have been, and that continue to be, transferred by Facebook Ireland (among others) to the USA. The core issue raised by High Court's questions is whether, notwithstanding such generalised access to the transferred data, a DPA is obliged, as a matter of EU law, to accept that the level of protection for the privacy of such personal data remains adequate, in circumstances where the data is being transferred by data controllers that it supervises within the EU (*i.e.* Facebook Ireland in the case of the DPC in the main proceedings). The applicant submits that such possibility of 'mass and undifferentiated' access results in wholly inadequate protection of sensitive, personal data in view of the criteria established in Article 25(2) and (6) of Directive 95/46/EC due to the possibility of serious violations of his rights under Articles 7 and 8 of the CFR and Article 8 of the ECHR against which there is no adequate remedy, since *de jure* and *de facto* the SHD's provisions amount to depriving him of his right to an effective remedy protected as general principles of EU law and in Article 47 CFR.

II. LEGAL AND FACTUAL BACKGROUND

A. Factual context and order of reference of High Court

3. The applicant is an Austrian national resident in Vienna. Since 2008, he has been a user of the social media service 'Facebook', and, when establishing his Facebook

³ Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce; OJ (2000) L 215, p 7.

⁴ The data that have already been transferred include highly personal and sensitive data including regarding the applicant's sexual orientation and voting intentions.

'account', he, like other Facebook users in Europe, was "required to enter into an agreement with Facebook Ireland Ltd.", which, as the High Court has found, means that Facebook Ireland falls "to be regulated by the [DPC] under the terms of the [Irish] Data Protection Acts 1988-2003".⁵ The High Court has further critically found that "some or all data relating to Facebook subscribers resident within the EU/EEA is in fact transferred to and held on servers which are physically located in the United States".⁶

4. Thus, the respondent DPC in the main proceedings is responsible for supervising Facebook Ireland, which controls (Article 2(d) of Directive 95/46) the data of its users. Facebook Ireland processes this data by transferring some or all of the data to servers situated at data centres that are physically located in the USA, where the data is processed by Facebook Inc. ("Facebook USA", the 'processor' under Article 2(e) of Directive 95/46). Accordingly, the impugned decision of the DPC has implications for the millions of 'Facebook' users, who, like the applicant, may be concerned by the possibility of accessing of their personal data by US security agencies under programmes and legislation such as the 'PRISM' programme and the 'FISA'.⁷
5. On learning of the revelations on the activities of the NSA, the applicant lodged a written complaint on 25th June 2013 with the DPC requesting termination of data transfers by Facebook Ireland to the US. This complaint was based, among other claims, on the rules governing data transfers to the USA under the SHD and the underlying Article 25 of Directive 95/46/EC,⁸ as well as on his fundamental rights under Articles 7 and 8 CFR and Article 8 ECHR. Mr. Schrems submitted that there was a high likelihood that US authorities had used their powers under various US laws, including the FISA to gain access to data held on servers of Facebook USA (amongst other companies). The Applicant contended that it was apparent from the FISA that processors, such as Facebook USA, must make all personal data available in bulk once they receive a non-specific 'directive' to cooperate with relevant US security authorities. The applicant submitted that Facebook Ireland⁹ had breached its obligations under Directive 95/46, as well as under the Irish Data Protection Acts 1988-2003 (which, *inter alia*, transpose that Directive into Irish law), by proceeding to transfer, and continue to transfer, his personal data to a country that does not provide an adequate protection. As the High Court has found, such transfers "facilitate[e] the processing of such data by Facebook itself".¹⁰ Although constitutional protection of the right to privacy in the United States 'Bill of Rights'

⁵ *Ibid.*

⁶ Para. 2 of the order for reference and para.17 of the judgment of 18 June 2014.

⁷ Paras. 10 to 12 of the judgment of 18 June 2014. The FISA is the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C., Ch. 36).

⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ (1995) L 281, p 31.

⁹ Para. 29 of the judgment of 18 June 2014.

¹⁰ Para. 29 of the judgment of 18 June 2014.

only applies to citizens and permanent residents of the United States (or to non-residents, such as previous residents, who maintain a substantial connection with the US) ("US persons"), the applicant, who is not such a person, contended that, in any event, even US persons have no right to address the relevant 'FISA court', which operates on an *ex parte* and secret basis.¹¹ Thus, there is no protection of his personal data and no factual or theoretical form of judicial redress against mass generalised surveillance in the US. The referring court considered such generalised access as demonstrating: "*almost beyond peradventure – that the US security services can routinely access the personal data of European citizens which has been so transferred to the United States and, in these circumstances, one may fairly question whether US law and practice in relation to data protection and State security provides for meaningful or effective judicial or legal control*".¹²

6. Instead of investigating the applicant's complaint, the respondent DPC first argued that he had no duty to investigate complaint. Later in the proceedings he invoked s. 10(1)(a) of the 1988 Act to find that the complaint cannot succeed on legal grounds ("frivolous and vexatious" in the technical sense of that provision), which allowed him to reject it without investigation. As interpreted by the High Court, this provision effectively connects the fact that a complaint 'cannot succeed' on legal grounds, with the option for an *in limine* rejection of it and the end of any investigation by the DPC. According to the DPC, s. 11(2)(b) of the 1988 Act, as amended, requires that the question of the adequacy of the level of data protection in a third country be determined in accordance with the findings of the Commission under Article 25(6) of Directive 95/46. The DPC considered that the Commission had thereunder adopted a favourable decision with regard to the USA, to the effect that US companies that participate voluntarily in the so-called 'Safe Harbor' programme ensure an 'adequate level' of data protection regarding the data in their possession, and that this included undertakings such as Facebook USA. Thus, the DPC regarded himself as being obliged (under s. 11(2)(a) of the 1988 Act, as amended) to accept the adequacy of data protection under the 'safe harbor' system and summarily dispose of the applicant's complaint, on the basis that the complaint, if investigated, could not succeed. The DPC, furthermore, considered that the applicant lacked *locus standing* to bring the complaint, because there was no evidence that his personal data had actually been accessed by the NSA or other US security agencies.
7. The applicant challenged the aforesaid DPC decision by way of the within judicial review proceedings initiated in October 2013. The relief he seeks therein from the High Court of Ireland is a declaration that the DPC's refusal to investigate his complaint is unlawful, as well as orders compelling the DPC to investigate the complaint and quashing the decision refusing to do so. Following the initiation of his judicial review application, the applicant lodged online complaints before the US

¹¹ This contention has been upheld by the High Court; see para. 7(b) of the order for reference.

¹² Para. 42 of the judgment of 18 June 2014; see also para. 7(b) of the order for reference.

Federal Trade Commission (“FTC”) and TRUSTe Inc. (“TRUSTe”, the dispute resolution body chosen by Facebook USA under the SHPs), concerning the available access by US authorities to data held with regard to him by Facebook USA.¹³ Unsurprisingly, since for the reasons developed further below both bodies lack jurisdiction to deal with such complaints, TRUSTe responded by stating that it does not have any jurisdiction in this case, while the FTC has not responded.¹⁴

8. In its judgment of 18 June 2014, which underlies its order for reference, the High Court first rejected (paragraphs 41-45) the DPC’s *locus standi* objection. It held that, even if the applicant cannot prove that his personal data has actually been accessed in the United States, he is “*entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only limited protection against any interference with that private data by the US authorities*”. The issue of standing to complain regarding the access available by US security agencies to his personal data has, therefore, been conclusively determined, for the purpose of this reference, in favour of the applicant by the High Court.
9. The High Court then considered the applicant’s position under national law with regard to the protection of the applicant’s right to privacy.¹⁵ It held that, under Irish constitutional law, for an interference with the right to privacy and, in particular, with the inviolability of the dwelling (which is engaged because, as found by the High Court, much of the private data at issue is generated within the home), it must be proportionate. However, the “*mass and undifferentiated*” accessing of personal data, such as that issue in the main proceedings, “*would not pass any proportionality test or could survive constitutional scrutiny on this ground alone*”.¹⁶ Accordingly, the referring court held that, “*if this matter were governed by Irish law, then measured by these particular constitutional standards, a significant issue would arise as to whether the United States ensures an adequate level of protection for the privacy and fundamental rights and freedoms, within the meaning of s. 11(1)(a) of the 1988 Act, such as would permit data transfers to that country*”.¹⁷ Thus, if Irish law alone were applicable, the High Court has held that the applicant’s judicial review application would succeed, since “*the [DPC] could not properly have exercised his s. 10(1)(a) powers to conclude in a summary fashion that there was nothing further to investigate*”.¹⁸
10. However, the referring court considered that the dispute in the main proceedings is only partially governed by Irish law, and that one “*must therefore turn to a consideration of the position at EU law*”.¹⁹ This was because s. 11(2)(a) of the 1998

¹³ See Annexes A.2 and A.3 to these observations.

¹⁴ *Ibid.*, at Annex A.2.

¹⁵ Paras. 47 to 57 in particular of the judgment of 18 June 2014.

¹⁶ Para. 12 of the order for reference.

¹⁷ Para 14 of the order for reference, and para. 56 of the judgment of 18 June 2014.

¹⁸ *Ibid.*, para. 12 of the order for reference.

¹⁹ Para. 57 of the judgment of 18 June 2014.

Irish Act effects “a renvoi” of the wider question of the adequacy of protection for the privacy of personal data in favour of EU law, while s. 11(2)(b) thereof obliges the DPC to determine the question of that adequacy in a third country, like the USA, “in accordance with a Community finding made by the European Commission pursuant to Article 25(6) of [Directive 95/46]”²⁰. The High Court further held that Article 3(1)(b) of the SHD does not apply in this case, because: “While Article 3(b) of the Safe Harbour Decision allows the national authorities to direct an entity to suspend data flows to that third country, this is in circumstances where - unlike the present case - the complaint is directed to the conduct of that entity”.²¹

11. With regard to EU law, the High Court therefore considered the nub of the issue to be whether the DPC is bound, by the finding contained in the SHD concerning the adequacy of protection provided for data subjects like the applicant that is available in the USA. The High Court held that, “the essential question which arises for determination is whether, as a matter of European Union law, the [DPC] is nonetheless absolutely bound by the finding of the European Commission as manifested in the [SHD] in relation to the adequacy of data protection in the law and practice of the United States having regard in particular to the subsequent entry into force of Article 8 of the Charter, the provisions of Article 25(6) of the 1995 Directive notwithstanding”.²² In this respect, the High Court considers that the applicant’s real objection concerns not the conduct of Facebook Ireland, as such, but “the fact that the Commission has already determined that US law and practice provided adequate data protection in circumstances where it is clear from the Snowden disclosures that personal data of EU citizens so transferred to the US can be accessed by the US authorities on a mass and undifferentiated basis.”²³

B. Core applicable EU law provisions

(i) Right to privacy, data protection, an effective remedy and to a fair trial

12. The right to privacy and data protection is protected under Articles 7 and 8 of the CFR. In cases arising prior to the entry into force of the CFR, from the general principles of Union law (Article 6(3) TEU). Article 6(3) TEU further provides that the “constitutional traditions common to the Member States” and the fundamental rights guaranteed by the ECHR “constitute general principles” of EU law. Specifically, with regard to the protection of personal data, Article 16(1) TFEU explicitly and unequivocally provides that: “Everyone has the right to the protection of personal data concerning them.” Protection is offered against public and private infringements.

²⁰ Para. 16 of the order for reference.

²¹ Para. 19 of the order for reference.

²² *Ibid.*, in the quotes from paras. 69-70 of the judgment of 18 June 2014 (emphasis in original).

²³ Para. 19 of the order for reference.

13. It is firmly established, that these fundamental rights place a duty on Member States and the Union reasonably to protect data subjects against violations by third parties. In addition to the substantive right to protection, Article 8(3) CFR also guarantees the procedural right to the supervision by an independent authority. The Court has held, in this regard, that: *"It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions"*.²⁴
14. The right to an effective remedy is protected under Article 47 CFR, and by Article 6(3) TEU in combination with Article 6 ECHR.²⁵ It is a general principle of EU law which comprises an essential component of ensuring respect for the rule of law (Article 2 TEU).²⁶ It is explicitly recognised and has been restated as the right to an 'effective remedy before a tribunal' in Article 47 CFR.

(ii) *Directive 95/46*

15. Under Article 1(1) of Directive 95/46, the objective of the Directive is stated to be the protection of *"the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"*.
16. Chapter IV, comprising Articles 25-26, of Directive 95/46 is concerned with the 'Transfer of Personal Data to Third Countries'. The principles governing such transfers are set out in Article 25. Article 26 of Directive 95/46 requires that *"Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place"*, once certain conditions are met amongst which, at indent (d), is the condition that *"the transfer is necessary or legally required on important public interest grounds"*.
17. Member States are required, under Article 25(1), to ensure in respect of transfers of personal data *"which are undergoing processing or are intended for processing after transfer"* is that *"the third country in question ensures an adequate level of*

²⁴ Case C-518/07 *Commission v Germany* [2010] ECR I-1885, para. 25.

²⁵ The Court has repeatedly found this right to be a fundamental right of individuals resulting from the common constitutional traditions of the Member States and recognised in Articles 6 and 13 ECHR. The fundamental rights arising from this are, thus, also protected as general principles of EU law under Article 6(3) TEU: see e.g.: Case 222/84 *Johnston* [1986] ECR 1651, paras 18 and 19; Case 222/86 *Heylens and Others* [1987] ECR 4097, para 14; Case C-424/99 *Commission v Austria* [2001] ECR I-9285, para 45; Case C-50/00 P *Unión de Pequeños Agricultores v Council* [2002] ECR I-6677, para 39; Case C-467/01 *Eribrand* [2003] ECR I-6471, para 61; Case C-432/05 *Unibet* [2007] ECR I-2271, para 37; Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakat* [2008] ECR I-6351, para 335; Case 12/08 *Mono Car Styling* [2009] ECR I-6653, para 47; Joined Cases C-317/08 to C-320/08 *Alassini* [2010] ECR I-2213, para 61.

²⁶ The recognition of which in the Union legal order dates back to Case 294/84 *Les Verts* [1986] ECR 1339, paras 23, 24. The relation between the right to an effective judicial remedy and the rule of law is outlined in Case C-50/00 P *Unión de Pequeños Agricultores v Council* [2002] ECR I-6677, paras 38-39.

protection". With regard to the required adequacy, Article 25(2) provides that:

"The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

18. The Commission is given a specific role under Article 25(4) and (5), where it "finds" that "a third country does not ensure an adequate level of protection within the meaning of [Article 25(2)]" of entering into negotiations "with a view to remedying the situation". Article 25(6) then provides:

"The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals."

Member States shall take the measures necessary to comply with the Commission's decision."

(iii) Commission Decision 2000/520/EC of 26 July 2000 ("the SHD")

19. Under Article 1(1) of the SHD:

"For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the 'Safe Harbor Privacy Principles' (hereinafter 'the Principles'), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter 'the FAQs') issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce".

The list of documents refers to four documents contained in Annexes III to VI of the SHD.

20. Under Article 3(1) of the SHD, the competent DPAs:

"may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the

FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

...

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond."

C. Questions referred & provisional view of High Court

21. In its judgment of 18 June 2014, the High Court decided to adjourn the proceedings before it and refer two questions pursuant to Article 267 TFEU, which it subsequently formulated in the order for reference. In doing so, it has defined the core issue of Union law underlying the reference as being whether, having regard to its "*findings of fact regarding the Snowden disclosures and the subsequent entry into force of Article 7 and Article 8 of the Charter*", as well as this Court's recent judgment in *Digital Rights Ireland*,²⁷ the DPC was bound by the determination made by the Commission in the SHD "*as to the adequacy of the data protection offered by US law and practice*", or may it, particularly in the light of the subsequent entry into force of the CFR, look "*behind that Community finding*" or even "*disregard*" it.²⁸
22. Prior to making the reference, the High Court heard an application, on 2nd July 2014, from Digital Rights Ireland to intervene in this case as an *amicus curia*, to which application it acceded on 16th July 2014.²⁹ By order of the same date, the High Court ordered that the two questions set out immediately below be referred to this Court.

"Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission

²⁷ Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v. Minister for Communication Marine and Natural resources & Others and Kärntner Landesregierung and Others* (Grand Chamber) ECLI:EU:C:2014:238 of 8 April 2014.

²⁸ Para. 21 of the order for reference, and paras. 70 and 84 of the judgment of 18 June 2014.

²⁹ It also acceded, on 16 July 2014, to an application made by Mr. Schrems, on 4 July 2014, for a 'protective costs order'. Thus, the High Court has ordered, for the applicant's benefit, that he be limited to a maximum of €10,000 costs in the proceedings should be ultimately not succeed and costs be awarded against him, although the High Court indicated that it would be unlikely that costs would be awarded against the applicant given the clear public interest of the issues raised by his judicial review application.

Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C364/012), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding?

Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?"

23. The High Court sets out its provisional views as to the possible responses this Court might give to the questions referred in the final section (paragraphs 23-27) of its order for reference. It considers it difficult to see how the SHD, at least viewed in the abstract, could satisfy the requirements of Articles 7 and 8 of the CFR, especially having regard to the principles enunciated in *Digital Rights Ireland*,³⁰ given the potentially generalised access by the US authorities to personal data transferred to the USA without any oversight having been carried out within the EU prior to the transfers taking place. Furthermore, the guarantee of the inviolability of the home as a "place of repose from the cares of the world" would, the High Court considers, be compromised, "if it were thought that electronic communications often emanating within the home could be accessed by State authorities ... on a casual or generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individual or individuals concerned and attended by appropriate and verifiable safeguards."³¹ Finally, the High Court observes that this Court might consider, in the light of *Digital Rights Ireland*, whether an interpretation of Directive 95/46, and especially of Article 25(6) thereof along with the SHD, would be open, such as would effectively permit a DPA, like the DPC in this case, not to be bound by the SHD and allow it to investigate whether privacy protection in the US satisfies the requirements of Articles 7 and 8 of the CFR.

III. ANALYSIS

A. Overview

24. It is clear from the order for reference that the key question raised is whether the administrative finding made by the Commission in the SHD to the effect that self-certification under the SHPs provides adequate protection of the personal data transferred from the EU to servers situated within the jurisdictional control of the US authorities remains valid. This question has arisen in circumstances where it has become clear within the last 18 months that the personal data so transferred to the US is accessible by the US authorities on a "mass and undifferentiated" basis without any effective legal remedy.

³⁰ Joined Cases C-293/12 and C-594/12, loc. cit., n. 27 above.

³¹ Para. 24 of the order for reference.

25. The applicant submits that there can only be one answer to this core question that would vindicate his fundamental rights, *i.e.* that Union law does not preclude DPAs, like the DPC in the main proceedings, from investigating and making findings on foot of complaints that third countries to which data are transferred from the EU do not respect fundamental rights guaranteed under Union law. The applicant's case is not, however, that there can never be access to such transferred data. Instead, he submits that such access cannot, under Union law for the specific reasons developed below, be countenanced where it occurs "*on a casual or generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individual or individuals concerned and attended by appropriate and verifiable safeguards*".³²
26. In the light of the High Court's findings of fact with regard to the access by US security agencies to data transferred to the USA, the principles relating to the fundamental right to privacy and data protection that this Court so cogently confirmed in *Digital Rights Ireland* with regard to data retention within the Union apply even more forcefully to data transferred to third countries whose authorities are outside the control of Union law.³³ In particular, the applicant submits that this Court should confirm the fundamental nature of the right to privacy and data protection in EU law, and in particular that this right may not be derogated from by the Commission when considering the adequacy of the laws and practices of third countries with regard to protecting the privacy and protection of personal data transferred to such countries.
27. Overall, the level of protection afforded to the applicant should not be lower under Directive 95/46, as further implemented by the SHD, than is required under the CFR. Moreover, it would be a highly regressive step for European integration if the referring court were precluded from vindicating the applicant's rights to privacy and data protection under Irish constitutional law due to a dramatically lower standard of protection being applicable under EU law on foot of an administrative assessment made over 14 years ago by the Commission in the SHD as to what constitutes adequacy of protection. In this respect, the applicant observes that a similar right to privacy to that he enjoys under Irish constitutional law is recognised under Austrian constitutional law.³⁴
28. By way of introduction, the applicant submits that DPAs, like the DPC, cannot, under

³² This Court has confirmed in a consistent line of case-law stretching from Case 6/64 *Costa v ENEL* [1964] ECR, English special edition, p. 585, the division of jurisdiction between it and national courts in the preliminary reference procedure between. As it held more recently, for instance, in Case C-140/09 *Traghetti del Mediterraneo* [2010] ECR I-5243, "[it] has no jurisdiction to give a ruling on the facts in an individual case or to apply the European Union law rules which it has interpreted to national measures or situations, since those questions are matters for the exclusive jurisdiction of the national court" (at para. 22, emphasis added). Thus, in the context of this preliminary reference procedure, the facts are exclusively for the national court to determine.

³³ Joined Cases C-293/12 and C-594/12, *loc. cit.*, n. 27 above.

³⁴ See, in particular, the judgment of the Austrian Constitutional Court on 'Data Retention', G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36 of 27 June 2014.

Article 3(1)(b) SHD, protect his rights and those of other Facebook users by suspending the data flows from Facebook Ireland to Facebook USA. Article 3(1)(b) requires four cumulative conditions to be fulfilled before a data flow suspension may be directed by a DPA,³⁵ of which the applicant considers the first cannot be fulfilled. That first condition of Article 3(1)(b), like the ‘chapeau’ of Article 3(1) SHD, refers to a violation of “the Principles” (in capital letters). The principles are defined in Article 1(1) of the SHD as the SHPs “*set out in Annex 1 to this Decision*”. This means that Article 3(1)(b) expressly refers to the SHPs in the annexed text, rather than any other (general) legal principles of EU law. Facebook USA, as a self-certifying body to which data are transferred has not itself violated the SHPs as a result of the ‘mass and undifferentiated’ access to the data it holds by US authorities, as the SHPs are expressly limited by US law, which paragraph 4 in Annex I to the SHD defines by reference to statute, government regulation, or case law. The crucial point is that the SHPs are not themselves EU law principles, but merely an annexed foreign legal text. The SHD is best described as a mere European ‘wrapper’ over inherently US legal texts, namely the FAQs and letters in Annexes I to VII to the SHD. An interpretation of the annexed text in the light of EU law would be inconsistent with the legal nature of the ‘Safe Harbor’ system, which is simply a US self-certification programme, recognised by the Commission. Interpreting this US system under EU law, would be like reinterpreting the law of other sovereign countries (which were found ‘adequate’ by the Commission) under Union law, while these countries are naturally following their own interpretation.³⁶

B. Invalidation of the SHD

29. The applicant submits that the SHD should be found invalid by this Court for the following reasons:

(i) *Incompatibility of the SHD with Article 25 of the Directive 95/46*

30. The SHD is incompatible with Article 25(6) of Directive 95/46, its legal basis. Firstly, it does not comply with the conditions of the provision, which allow the Commission to find that a third country such as the USA “*ensures adequate protection*” by reason “*of its domestic law or of the international commitments it has entered into*”. The Commission thereby has to assess the level of protection provided in a third country. It has to take into account, in particular, factors such as the legal and factual level of protection. For the reasons developed in detail by Professor Böhm

³⁵ That the conditions are cumulative is, the applicant submits, clear from the punctuation of the provision (the use of semi colons after each condition) and the use of “*and*” by way of introduction to the fourth condition. The cumulative nature of the conditions also emerges equally clearly from at least the French and German texts of Article 3(1)(b) SHD.

³⁶ The High Court has reached the same conclusion as to the non-applicability of Article 3(1)(b) of the SHD in this case, but on foot of different reasoning: see para. 10 above.

in her opinion contained in Annex 1 to these observations, the applicant submits that the Commission could not reasonably have formed its opinion in the SHD in July 2000 to an adequate level of protection based on the SHPs in combination with existing US domestic law.³⁷ The differences in levels of protection provided by EU law, on one hand, and by the SHPs regime, on the other, are, the applicant submits, by reference to Professor Böhm's analysis in her opinion in Annex 1, so numerous and substantially so serious to allow rationally for a finding of adequacy. The Commission therefore committed a manifest error of assessment which would justify this Court invalidating the SHD. In support of this submission, the applicant would, in particular, refer the Court to the following reasons.

31. Firstly, the conditions of Article 25(6) Directive 95/46 were not fulfilled. In order to adopt the SHD on the basis of the SHPs, the Commission must have understood the SHPs as "*international commitments*" entered into by the US under Article 25(6) following negotiations under Article 25(5) of Directive 95/46. However, it is submitted that the 'safe harbor' regime (comprised of the SHPs and the 'Frequently Asked Questions' ("FAQs")) do not amount to an international commitment by the US Government, but merely to a publication of a US government department (the US Department of Commerce) that offers a code of behaviour allowing private parties to engage in more or less supervised commitments on their part as to the protection and security of the personal data they control under a self-certification structure that is primarily supervised by private arbitration.
32. In essence, individual private companies and organisations can voluntarily declare that they intend to comply with the code in their capacity as data controllers. This cannot constitute "*an adequate level of protection ... by reasons of [the US's] domestic law or of the international commitments it has entered into*" (emphasis added) for the purpose of Article 26(6) of Directive 95/46. Consequently, the applicant submits that the Commission erred in law in concluding that it was entitled to make a finding of adequacy in the SHD on the basis of Article 25(6). The finding of adequacy in the SHD decision is, thus, invalid and not binding on DPAs like the DPC.
33. Secondly, and more substantively, the applicant submits that the SHD and the SHPs fall short in view of regulatory content. Thus, Directive 95/46 defines in Article 2(b), as modes of processing of data: "*any set of operations, which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*" The SHD limits, by stark contrast, only the transfer to a third party and the change of purpose. Any other form of

³⁷ An in-depth analysis of the inadequacy of the SHD by comparison to EU data protection law is set out, for the assistance of the Court, in the opinion of Prof. Dr. Franziska Böhm of the University of Münster (Germany): see Annex A.1.

processing, even of data of the most personal and thus sensitive nature, can be processed without meaningful limitations. The applicant submits that the SHD is therefore incapable of providing an adequate level of protection in the sense of Article 25(1) and (2) of Directive 95/46.

34. Consequently, the applicant submits that the Commission erred in law in concluding that it was entitled to make a finding of adequacy in the SHD on the basis of Article 25(6). The finding of adequacy in the SHD decision is thus invalid and not binding on DPAs like the DPC.

(ii) *Incompatibility of the SHD with fundamental rights protection in EU law*

35. It is appropriate initially to recall that the High Court has already found that the standard of protection of privacy currently available to the applicant in the context of the existing SHD is grossly inadequate compared with the protection of the right of privacy the applicant enjoys as a fundamental right under Irish constitutional law. Furthermore, the applicant submits that, as an Austrian national and resident, he also enjoys rights under the Austrian constitutional law, which recognises and applies the standard of privacy protected under Article 8 of the ECtHR and the right to data protection in section 1 of the Austrian *Datenschutzgesetz*, as directly applicable constitutional rights.³⁸ These standards would not permit the generalised accessing of personal data such as that issue in the main proceedings that has been found by the referring court to occur in the USA. The high level of protection of privacy that the applicant enjoys under national law in at least Ireland and Austria (amongst, in all likelihood the applicant submits, many other Member States) is a factor that he, respectfully submits, should be borne in mind by this Court in considering the scope of the protection of the privacy of his personal data under EU law, both under the CFR and under the general principles of EU law.

a) *Right to privacy under Directive 95/46*

36. Any measure taken on the basis of Directive 95/46 must comply with the standards of protection established by the EU-protected fundamental rights. Such rights arise both from the CFR (Article 6(1) TEU) and, in cases arising prior to the entry into force of the CFR, from the general principles of Union law (Article 6(3) TEU). Article 6(3) TEU further provides that the fundamental rights guaranteed by the ECHR “constitute general principles” of EU law. Specifically, with regard to the protection of personal data, Article 16(1) TFEU explicitly and unequivocally provides that: “Everyone has the right to the protection of personal data concerning them.”³⁹

³⁸ See the Austrian Constitutional Court’s ‘Data Retention’ judgment of 27 June 2014, cited in n. 34 above.

³⁹ In *Digital Rights Ireland*, the Court confirmed the close link between the CFR and the ECHR in data protection related cases.

37. According to Article 1(1) of Directive 95/46, its objective is to protect the “*fundamental rights and freedoms of natural persons, and in particular their right to privacy with regard to the processing of personal data*”. In this respect, it should also be noted that recital 10 in the preamble thereto states that “*the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in [Convention No. 108 of 1981].*”
38. The SHD, which is based on Article 25(6) of Directive 95/46, regulates the transfer of personal data to the USA, while the SHPs in Annex I thereto limit the subsequent use thereof of the data. The SHD therefore falls to be reviewed with regard to its compliance with the requirements of Articles 7 and 8 CFR, which fall to be interpreted, as this Court has held in *Digital Rights Ireland*, in a parallel way to the requirements flowing from Article 8 ECHR.

b) Scope of right to privacy with regard to processing of personal data in EU law

39. It is clear from Articles 7 and 8 CFR that protection of personal data is offered as against both public and private infringements. This is clear from the wording of Article 8 CFR, which calls for an independent supervisory authority (Article 8(3)) to review potential infringements, and from the formulation of Article 8(2) CFR, which makes clear that both public and private infringements of the right are within the scope of protection. The applicant submits that the express right to the protection of personal data specified in Article 16(1) TFEU has the same scope.
40. According to the requirement of minimal protection in Article 52(3) CFR, the rights flowing from Articles 7 and 8 CFR fall to be construed as containing the minimum level of protection required by Article 8 ECHR, which guarantees, amongst others, the right to respect for private and family life. The rights defined in Articles 7 and 8 CFR are a restatement of the rights accepted as general principles of EU law as they were in force at the time of the adoption of Directive 95/46 and the SHD in 2000. The two sources of fundamental rights protection may therefore be treated together in the discussion of privacy and the protection of personal data.
41. It is well established that the processing of data is covered by both the right to privacy and the right to the protection of personal data under Articles 7 and 8 CFR.⁴⁰ In fact, the right to the protection of personal data has its roots in the protection of privacy. Thus, in *Digital Rights Ireland*, the Court held that “*the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of*

⁴⁰ See Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paras 47, 52; and Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, loc. cit. n. 27 above, para 29.

the Charter".⁴¹ The Court explained its approach as follows in the *Schwarz* case:

*"Article 7 of the Charter states, inter alia, that everyone has the right to respect for his or her private life. Under Article 8(1) thereof, everyone has the right to the protection of personal data concerning him or her. It follows from a joint reading of those articles that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights. From the outset, it should be borne in mind that the right to respect for private life with regard to the processing of personal data concerns any information relating to an identified or identifiable individual."*⁴²

42. With regard to the notion of interference of these rights, the Court has held that, to establish the existence of an interference with the fundamental right to privacy under Article 7 CFR, *"it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way"*: the communication of collected personal data to third parties, be they public authorities or private parties, constitutes interference with the right to privacy, *"whatever the subsequent use of the information thus communicated"*.⁴³ Furthermore, in *Digital Rights Ireland*, the Court confirmed that, permitting access by competent national authorities to such data, constitutes an additional, discrete interference with that fundamental right.⁴⁴ Moreover, any form of processing of personal data is protected by Article 8 CFR and constitutes an interference with this right.⁴⁵ Given the nature of exchange between friends and family on Facebook, and that such data includes personal information, the applicant submits that the review of the Commission's assessment as to the adequacy of protection in the SHD should be carried out against the combined criteria of Articles 7 and 8 CFR.
43. Interference by processing takes place in various contexts. Facebook USA processes personal data by storing and using the data of its users for commercial purposes. The company establishes user profiles and sells some results of the analysis of profiles to clients. Furthermore, Facebook Ireland processes data by transferring the users' personal data (such as photos, mails and messages, bibliographical data and social relations, expressions of 'likes' or 'following' of sources of information) to the data centres of its parent company, Facebook USA, in the USA⁴⁶ For the purpose of the

⁴¹ *Ibid.*, para 53.

⁴² Case C-291/12 *Michael Schwarz v Stadt Bochum* ECLI:EU:C:2013:670 of 17 October 2013, paras. 24-26, citing Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert*, loc. cit, n. 39, para. 52, and Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD* [2011] ECR I-12181, para. 42.

⁴³ Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk & Others* [2003] ECR I-4989, paras. 74-75.

⁴⁴ *Digital Rights Ireland*, at para. 35. The Court referred to Article 8 of the ECHR, and the ECtHR case-law in *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI).

⁴⁵ *Digital Rights Ireland*, at para. 36.

⁴⁶ Transfer of data constitutes processing in EU law. Thus, Article 2(b) of Directive 95/46 defines 'processing of personal data' (processing) as: *"any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making*

complaint at issue in the main proceedings the central matter is the transfer of data from Facebook Ireland to Facebook USA, in the light of the generalised accessibility of the data stored at Facebook USA to the NSA and other US security agencies under powers they enjoy under domestic US legislation.⁴⁷

44. The issue which arises is not dissimilar to but more serious than that considered by the Court in the *Digital Rights Ireland* with regard to the Data Retention Directive.⁴⁸ In that case, the Court held that the interference was a particularly serious one, because of the wide-ranging consequences and because the persons concerned were not informed of the processing, which could create “*in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*”.⁴⁹ In this case, the interference is far graver as the data at issue is being transferred beyond the protection of EU law, and:

- At least all non-US Facebook users are concerned, amongst them the applicant.⁵⁰
- European users remain largely uninformed about the fact that their individual data, including the content of their ‘private’ conversations, will be generally accessible by US security agencies.
- Although such users signed the general terms and conditions with Facebook, those terms do not specify that their personal data has been or will be accessed by US security agencies in specific cases, such that European Facebook users could not expect that their posts, for instance, could be routinely accessed by the NSA in the context of mass and undifferentiated access.⁵¹
- The amount of the data concerned is enormous and this, combined with the secret access by the NSA and others, renders the interference extremely serious.
- The referring court has found that within the USA, for data transferred from Facebook Ireland, “*EU citizens have no effective right to be heard on the question of the interception and surveillance of their data*”.⁵² The relevant ‘FISA court’ operates “*on an ex parte and secret basis. EU citizens have no effective right to be heard on the question of the interception and surveillance of their data*”.⁵³

available, alignment or combination, blocking, erasure or destruction” (emphasis added).

⁴⁷ Most notably, under s. 215 of the Patriot Act, s. 702 of the FISA, as amended, and Presidential Executive Order 12333.

⁴⁸ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

⁴⁹ Para. 37.

⁵⁰ It appears from Facebook’s commercial claims that 82% of its users are outside of the US and Canada. It is, therefore, likely that the personal data of all such users is managed (and thus transferred to Facebook Inc in the US) by Facebook Ireland.

⁵¹ The relevant US law does not require probable cause or other reasons to access the information, which could potentially satisfy the requirements set out in *Digital Rights Ireland*, at paras. 39- 40.

⁵² Para. 7(b) of the order for reference.

⁵³ Para. 7(b) of the order for reference. By contrast, in *Digital Rights Ireland*, this Court held (para. 62) that “*above all*” one of the failings of the Data Retention Directive was that access by the DPAs to the data retained was “*not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary*”.

c) Limitation of rights guaranteed by Articles 7 and 8 CFR

45. Any limitation of the rights established by Articles 7 and 8 CFR requires justification under the criteria of Article 52(1) CFR. Accordingly, limitations must "*be provided for by law and respect the essence of those rights and freedoms.*" Furthermore, limitations have to be proportionate and may be made to rights protected under Articles 7 and 8 CFR "*only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*"⁵⁴ The applicant submits that the interference involved does not respect the essence of the rights at issue and is manifestly disproportionate.
46. In *Digital Rights Ireland*, the Court clarified that the essence of Article 7 CFR comprises "*the acquisition of knowledge of the content of the electronic communications as such*". Accordingly, the essence of Article 8 CFR is violated when a person is stripped of any protection of personal data, especially if none of the conditions of Article 8(2) CFR, *i.e.* of purpose specification, access to collected data and rights of rectification, is fulfilled. In *Weber and Saravia v. Germany*, the ECtHR recognised the importance of a notification in the context of surveillance measures, because it permits the individuals affected to be informed of surveillance measures and, if they wish, more effectively to challenge the legality of such measures; *i.e.*, effectively to exercise a remedy against such measures.⁵⁵ This Court has upheld in *Digital Rights Ireland* the importance of information as the minimum safeguard required to counter the concern of constant surveillance.⁵⁶
47. The US Government's programmes allow, according to the findings of the High Court, full-scale access to content information, including highly personal and sensitive information. Under US law, the NSA and other US security agencies have potential access to the content of all the transferred data. This is exacerbated by the secrecy of the 'PRISM' programme, and the prohibition under US law on participating organisations from informing data subjects about the accessing of their data, as well as by the fact that no probable cause is required before the US security authorities may deliver a 'directive' to a self-certified 'safe harbor' organisation like Facebook USA requiring bulk access to the data. Worse still is the fact that the US authorities, according to the Snowden disclosures, not only have access to the data stored at Facebook USA, but also to that at a vast number of other telecom, IT or internet providers. This personal information stems not only from the applicant's use of certain services, but may also be gathered by these services themselves, or submitted by third parties (e.g. other users of such services). Thus, systems like X-Keyscore, according to the findings of the High Court, allow the US authorities to

⁵⁴ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, at para. 38.

⁵⁵ No. 54934/00 of 29 June 2006.

⁵⁶ Para. 37.

access and merge this information. This results in vast amounts of personal information about most users of online services being available to the US authorities.

48. In summary, it is difficult to imagine more-clear cut and egregious violation of the essence of the rights to privacy and data protection in that neither privacy nor data protection is respected. Therefore, Article 25 of Directive 95/46 cannot be interpreted to allow the Commission to find a system which leaves the possibility of such violations of fundamental rights unsanctioned as an “adequate level of protection”. The applicant therefore submits that the SHD is invalid on these grounds.

d) Proportionality

49. The applicant further submits that the general accessibility to the NSA and other US security agencies of the transferred data of the applicant also constitutes a manifestly disproportionate interference with his right to privacy and data protection. It is well established that, to be proportionate under Article 52(1) CFR, a restriction or limitation must be necessary “*genuinely to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*”.⁵⁷ The Court has summarised the relevant requirements arising from Article 52(1) CFR for assessing proportionality as being that measures adopted by Union institutions “*do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued*”.⁵⁸
50. The Commission’s assessment under Article 25(6) Directive 95/46 of the adequacy of protection offered by third countries with regard to the level of protection afforded by Articles 7 and 8 CFR is based on factual assessments. In exercise of its mandate under Article 25(6) Directive 95/46, the Commission acts within a set of clearly defined criteria established by the Directive. It thereby adopts an administrative decision applying legislative criteria to a given set of facts. Such decisions are subject to full review by the Court as to the proportionality of the assessment, which in the main proceedings concerns the Commission’s assessment as to the adequacy of protection afforded by the US “*by reason of its domestic law or of the international commitments it has entered into*”.⁵⁹ The Court therefore has full jurisdiction to review the proportionality of the Commission’s assessment of the adequacy of the US legal protections. Furthermore, it is clear from *Digital Rights Ireland* that the protection of the fundamental right to respect for private life requires that “*derogations and*

⁵⁷ Case C-292/97 *Karlsson* [2000] ECR I-2737, para. 45.

⁵⁸ Case C-283/11 *Sky Österreich* (Grand Chamber), ECLI:EU:C:2013:28, para. 50.

⁵⁹ In addition to recognising the SHPs of the US Department of Commerce, the Commission has recognised, under Article 25(6) of Directive 95/46, Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and as providing adequate protection. Data transfers to all other third countries are governed by Article 26 of the Directive.

limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".⁶⁰ Moreover, the more serious the interference with the right to privacy the more reduced is the institution's discretion.⁶¹

51. In the main proceedings, the High Court has found the interference to be a high-end, extremely serious one involving the potential of "*mass and undifferentiated*" access by US security authorities of the personal data of Facebook users including the applicant following the transfer of their data to the USA.

Public Interest Pursued by the SHD

52. The public interest pursued by Article 25 of Directive 95/46 is to ensure such cross-border flows of personal data as "*are necessary to the expansion of international trade*", which recital 56 of Directive 95/46 states to be an objective of the Directive. The applicant submits, however, that it cannot be in the public interest pursued by Article 25 of Directive 95/46 or the SHD to allow data transfers to provide foreign intelligence information for espionage, national security or law enforcement purposes of a third country. Such data transfers are the subject of mutual assistance agreements.
53. Furthermore, it cannot be appropriate and necessary to permit extremely serious limitations of fundamental rights to ensure a marginally higher level of trade. In any case, the Commission nowhere indicated in the SHD why such limitations might be necessary and capable of fostering the trade-related objective of Directive 95/46. Instead, recital 4 of the SHD states as objective of the decision not to "*arbitrarily or unjustifiably discriminate against or between third countries where ... conditions prevail nor constitute a disguised barrier to trade taking into account the Community's present international commitments*". In brief, the applicant submits that the SHD clearly violates first condition of proportionality, which requires a measure be capable of achieving a legitimate public policy objective of the Union.
54. Moreover, recital 56 of Directive 95/46 states that: "*this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection*", and that "*the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations*". Those circumstances, of course, include the evidence accepted by the referring court of generalised access by US security authorities to transferred personal data. This access does not require any relationship between the access to the data and a specific concern for and a threat to public security. It does not, therefore, respect the principle of 'purpose limitation' in Article 8(2) CFR. There is no limitation on such generalised access: (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious

⁶⁰ *Digital Rights Ireland*, para 52: where the Court cited, *inter alia*, Case C-473/12 *IP I EU*:C:2013:715, para 39.

⁶¹ *Ibid.*, paras. 47-48.

crime; or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

55. Thus, the SHD, like the Data Retention Directive considered in *Digital Rights Ireland*, “fails”, by virtue of the letdown of the US law deemed to provide adequate protection in the SHD. The SHD fails “to lay down any objective criterion by which to determine the limits of the access ... to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference.”⁶² It thereby fails to provide for adequate protection
56. The SHD is also inappropriate to pursue its supposed purpose, by comparison to *Digital Rights Ireland*, because, given the structure of the SHD under which the application of US law is accepted by the Commission, the degree to which the fundamental right of European users of Facebook will be protected depends on the law of a third country that limits, according to a study commissioned by the European Parliament, the protection of the right to privacy under its own constitutional law to its own citizens and permanent residents.⁶³ Furthermore, the SHD Decision ignores the fact that not only private activity but also the activity of public authorities may be a source of violation of rights under Articles 7 and 8 CFR. It finds a system to be ‘adequate’ that allows for transfer of data in absence of substantive and procedural conditions relating to the access by the US security authorities to the transferred data and to their subsequent use thereof under US law. This clearly violates the principles enunciated in *Digital Rights Ireland* that objective criteria should be laid down by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued.⁶⁴ Those principles also require that such minimum safeguards be “specific and adapted to: (i) the vast quantity of data” which can be transferred; “(ii) the sensitive nature of that data”; and “(iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality”.⁶⁵ The applicant submits that the minimum requirements specified in *Digital Rights Ireland* (especially at paragraph 62) are the same as those that should apply in assessing whether adequate protection is afforded by third countries for rights protected under Articles 7 and 8 CFR.

⁶² *Digital Rights Ireland*, para. 60.

⁶³ See, for a synopsis of the situation in US constitutional law, Bowden/Bigo, “The US surveillance programmes and their impact on EU citizens’ fundamental rights”: study requested by the Committee on Civil Liberties, Justice and Home Affairs Committee of the European Parliament, September 2013.

⁶⁴ *Digital Rights Ireland*, para. 62.

⁶⁵ *Ibid.*, para. 66.

Limitation Strictly Necessary – Availability of Less Onerous Options

57. Limitations to fundamental rights of individuals are only **strictly necessary**, if no measures are conceivable that might limit the relevant fundamental rights to a lesser degree than the ones chosen. It is well established that compliance with the proportionality principle has to be, at least implicitly, explained in the reasoning of an EU act that limits fundamental rights. In this respect too, the SHD violates the principle of proportionality, whilst also suffering from a lack of reasoning under Article 296 TFEU. The reasoning needs to be sufficient to allow the courts to undertake a review of a decision. Thus, the statement of reasons “*must disclose in a clear and unequivocal fashion the reasoning followed by the Community authority which adopted the measure in question in such a way as to make the persons concerned aware of the reasons for the measure and thus enable them to defend their rights and to enable the Court to exercise its supervisory jurisdiction*”.⁶⁶ Compliance with proportionality – especially showing that the Commission has considered the means which least limits the rights of individuals – has to result from the text of the act and be generally indicated in its preamble.⁶⁷ However, the SHD is devoid of consideration as to possible alternatives involving less far-reaching limitations. Equally, no, even implicit, discussion of the consequences of the Decision for the protection of individual rights is offered. Consequently, it breaches the obligation to give sufficient reasons under Article 296 TFEU, and, in so doing, violates the principle of proportionality regarding the ‘least-onerous-measure’ test; since the Commission failed to indicate why the far-reaching limitations it implicitly endorses of individual privacy rights of the data subjects of European controllers users could be justified as **strictly necessary** to facilitate the free flow of their data to the USA.
58. Indeed, the contrary is in fact the case. In recital 5 to the SHD, the Commission declares itself effectively uncertain as to whether any of limitations under the SHPs are in fact the least onerous possible. Thus, the Commission admits that “*the adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles...*” (emphasis added). There was therefore merely an aspiration even when the SHD was adopted in July 2000 that the SHPs would actually achieve their objective. In that sense, and independently even of the revelations that have in the meantime emerged of the “*mass and undifferentiated access*” by US security agencies under the ‘PRISM’ program and the FISA to personal data that are transferred to the USA, the applicant submits that it was clear, even, *ab initio*, that the limitations on the right to privacy of all data subjects whose data would be transferred to the USA, by voluntarily participating and self-certifying organisations to the SHPs like Facebook Ireland, was not **strictly necessary**.⁶⁸

⁶⁶ Case C-269/90 *Technische Universität München* [1991] ECR I-5469, paras. 14 and 26.

⁶⁷ Case T-461/08 *Evropaiki Dynamiki* [2011] ECR II-0000, paras. 118-124.

⁶⁸ In fact, the Commission itself has documented violations of rights and other cases of malfunction of the SHD in its three implementing reports in 2002, 2004 and 2013 (see Commission documents SEK(2002) 196 of 13.12.2002 and SEC(2004) 1323 of 20.10.2004 and Commission document COM(2013) 847 final, of 27

59. The applicant submits that many less onerous ways to achieve the public interest in enhancing trade with the United States, which neither require that the applicant's fundamental rights to be rendered unenforceable nor that allow a foreign government to use personal data for mass surveillance, are imaginable. Thus, no adequacy decision could have been adopted, since trade with the US can also be fostered by decisions under Article 25(1) and (2), in combination with, where necessary, Article 26, of Directive 95/46. These provisions generally allow data transfers after individual analysis of adequacy or the application of exceptions listed in Article 26(1). In addition Article 26(2) allows the use of contractual clauses, binding corporate rules (BCRs) or other contractual instruments, e.g. for not strictly necessary but legitimate scenarios like the 'outsourcing' of processing operations to a third country. These instruments are used in relation to all trading partners of the Union, which do not provide 'adequate protection'. The only difference between Article 26 and Article 25(6) is that, under the later, there is a broad adequacy decision which results in an unlimited free flow of data, as occurs within the EEA, while Article 26 requires that one of the many exceptions in Article 26(1) or (2), which are subject to the scrutiny of the DPAs, be fulfilled. Allowing data transfers to the United States under supervision by DPAs and suspension of specific data flows if the fundamental rights of data subjects are, or are likely to be, violated would, thus, have been a far less onerous alternative to the SHD adopted under Article 25(6), which unduly limits the discretion of DPAs to take action if the fundamental rights of data subjects are in fact violated.
60. Another less onerous form of regulation, it is submitted, could have comprised the creation of criteria for the limitation of access by foreign authorities to data transferred from the EU to the US. In *Digital Rights Ireland* the Court criticised the Data Retention Directive for failing "*to lay down any objective criterion by which to determine the limits of the access ... to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference.*" The Commission could have introduced exceptions and limitations for excessive access by espionage, national security or law enforcement authorities. It could have achieved this by insisting on an "international commitment" by the US, as it did, e.g., for Passenger Name Records. This would have allowed the Commission to ensure minimal standards of protection and would have allowed it to take factual measures if the USA violated such an agreement

Overall Reasonableness

61. The SHD also fails the overall reasonableness test, *i.e.* the third test of proportionality,

November 2013). The November 2013 report is the most damning, insofar as it lists considerable weaknesses of the 'safe harbour' self-certification system and the consequences flowing therefrom for the protection of rights of individuals.

which concerns the overall control of the whether there is a balanced relationship between ends and means. With regard to validity of the SHD, it is the interest in free trade and the free flow of data with the USA that must be balanced with that of the protection of the data subjects' fundamental rights. Yet, the SHPs foresee far-reaching exceptions compared to EU data protection provisions. Potentially any provision of US law, government regulation or court ruling could unilaterally set aside all protection provided by the SHPs. This arises chiefly from the exception created by paragraph 4 of the SHPs in Annex I of the SHD. This results from the functioning of the SHD as a mere EU law 'wrapper', which, by declaring the adequacy of the US rules listed in the annex, aims at formally fulfilling the requirements of Article 25(6) Directive 95/46. Since paragraph 6 of Annex I to the SHD declares US law applicable to the SHPs, the exceptions or limitations on the right to privacy under the SHPs will fall, in principle, to be construed under US law alone. Thus, as a protection for EU citizens, the SHPs are little more than a chimera as regards fulfilling the requirements of Article 25(6) Directive 95/46.

62. However, this Court has consistently held that any acts of the Union institutions must comply with fundamental rights standards established by Union law. In *Kadi I*, for example, confirmed in *Kadi II*⁶⁹ the Court held that “*respect for human rights is a condition of the lawfulness of Community acts ... and that measures incompatible with respect for human rights are not acceptable in the Community*”.⁷⁰ Furthermore, it held that no provisions of public international law — and it is submitted that this is all the more true for the law or a self-certification programme of a foreign country — can “*be understood to authorise any derogation from the principles of liberty, democracy and respect for human rights and fundamental freedoms enshrined in Article 6(1) EU as a foundation of the Union*”.⁷¹ This reasoning, applied by analogy to this case, requires that the Commission’s adequacy decision under Article 25(6) of Directive 95/46 cannot result in data being transferred without further control to a foreign jurisdiction where they are effectively stripped of “*the guarantee of effective judicial protection*” assured by both the CFR and ECHR.⁷²

(iii) *Invalidity of the SHD for failure to ensure for control by an independent authority*

63. In *Digital Rights Ireland*, the Court held that “*above all*” one of the failings of the Data Retention Directive was that access by the competent national authorities to the data retained was “*not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data*”

⁶⁹ Joined Cases C-584/10P, C-593/10P and C-595/10P *United Kingdom & Others v Kadi* ECLI:EU:C:2013:518, para. 88.

⁷⁰ Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat* [2008] ECR I-6351, para. 284.

⁷¹ *Ibid.*, para. 303.

⁷² *Ibid.*, at para. 133 and for the ECHR see ECtHR No 10593/08, judgment of 12 September 2012 in *Nada v Switzerland*, at para. 211.

and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions". In this case, a further clear failing of the SHD is the comparable absence of provisions for control by an independent authority of compliance with the requirements of protection and security of personal data under Article 8(3) CFR. However, this is an express requirement under Article 39 TEU, under which rules adopted by Union institutions regarding the processing or free movement of personal data "*shall be subject*", with regard to compliance, "*to the control of independent authorities*". Furthermore, this requirement is repeated in Article 16(2) TFEU.⁷³

64. A definition of an independent supervisory authority is provided in recital 63 of Directive 95/46, which states that supervisory authorities "*must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals and powers to engage in legal proceedings*". This definition is based on the Council of Europe Convention No. 108 of 1981.⁷⁴
65. This Court has held that the independence of supervisory authorities is an essential component of the right to the protection of personal data. Ironically, this has been confirmed in infringement actions brought by the Commission against Germany and Austria for those Member States' failure to comply with their obligations under Directive 95/46.⁷⁵ In its complaint against Germany, the Commission contended that Germany was in breach of its obligations by not giving sufficient independence to its data protection supervisors. The Commission contended that an independent data protection supervisor is essential. The Court agreed. It held that the guarantee of the independence of national supervisory authorities: "*is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim*"; and that: "*It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions*".⁷⁶
66. The applicant submits that SHD manifestly fails to comply with this requirement. Within its annexes provision is made for a rather unique construct comprising essentially two elements: firstly, a voluntary regime of arbitration by private bodies, especially mentioning in FAQ 11 TRUSTe and BBBOnline; and, secondly, a possibility of referral of questions from these bodies to the FTC (see FAQ 11 in

⁷³ The importance of this requirement was stressed by the Court in Case C-614/10 *Commission v Austria* EU:C:2012:631, para. 36.

⁷⁴ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flows of 8 November 2001.

⁷⁵ Case C-518/07 *Commission v Germany* [2010] ECR I-1885, paras. 23-25, and Case C-614/10 *Commission v Austria* [2012] ECR I-0000, para 37.

⁷⁶ Case C-518/05, paras. 23-25 (emphasis added).

Annex 2 to the SHD).⁷⁷ The SHPs comprise a code of conduct to which companies can voluntarily subscribe. This is made public by a listing of such companies on a list maintained by the US Department of Commerce.⁷⁸ In case of disputes between a self-certified company and a consumer, dispute resolution is undertaken by private arbitrators, such as 'BBBOnline' and 'TRUSTe'. These private arbitration structures may only investigate complaints regarding the private activities of self-certifying companies. It is clear from FAQ 11 that they have no power to review the legality of activity of public authorities within the US. With regard to the FTC, it commits itself under FAQ 11 to reviewing, on a priority basis, referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the SHPs and to determine whether section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in commerce, has been violated.⁷⁹

67. The types of available review are explicitly designed to cover only the activities of undertakings which have self-certified themselves as coming under the SHPs. The FTC appears to have no jurisdiction to review possible violations of data protection principles of public actors, such as the US government or security authorities like the NSA.⁸⁰ Yet, this power is essential to guarantee fully effective data protection rights.
68. Accordingly, the Commission could not have found, in adopting the SHD, that, with regard to all the data that would be transferred to the US, there would be adequate protection for the right conferred by Article 8(3) CFR, *i.e.* effective provision for control to be effected by an independent authority of compliance with the requirements of protection and security of personal data.

(iv) Invalidity of the SHD due to incompatibility with the right to an effective remedy in EU law

69. The right to an effective remedy for violation of an EU-law protected right is assured by the CFR (especially Article 47) and by the general principles of Union law⁸¹ (*ubi*

⁷⁷ Other bodies offering such arbitration under the SHPs include the 'Direct Marketing Association Safe Harbour Programme', the 'Entertainment Software Rating Board Privacy Online EU Safe Harbour Programme', the 'Judicial Arbitration and Mediation Service (JAMS)' and the 'American Arbitration Association'.

⁷⁸ This list, however, is far from regularly updated and may contain companies which are no longer compliant with the voluntary code of conduct, or which have, despite self-certification, never fully complied. See the report of the German Federal Agency for Data Protection and Access to Information: Deutscher Bundesbeauftragter für den Datenschutz und die Informationsfreiheit at <http://www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html?nn=409532>.

⁷⁹ The FTC does not generally investigate complaints from data subjects like the applicant. It has no direct enforcement remedy but may merely find a violation of the SHP also violates s. 5 of the FTC Act.

⁸⁰ The applicant made a complaint to the FTC regarding the potential accessing of his personal data, as transferred to the USA by Facebook Ireland, by US security authorities; see Annex A.3.. He has not yet received a response to this complaint.

⁸¹ The Court has repeatedly found this right to be a fundamental right of individuals resulting from the common constitutional traditions of the Member States and recognised by Articles 6 and 13 of the ECHR. The fundamental rights arising from this are thus also protected as general principles of EU law under what is now

ius ibi remedium).⁸² It requires an effective remedy before a court to seek to challenge measures that restrict the right to privacy and the protection of one's personal data.

70. With regard to data protection, the applicant submits this means that persons whose data has been accessed or subject to surveillance measures need to be informed about this. This is a pre-condition for the possibility to exercise the right to an effective remedy. In *Weber and Saravia v. Germany*, the ECtHR explicitly recognised the importance of a notification in the context of surveillance measures, because it permits the individuals affected to be informed and, if they wish, more effectively to challenge the legality of such surveillance measures, *i.e.* effectively to exercise a remedy against such measures.⁸³ This Court has upheld in *Digital Rights Ireland* the importance of information as the minimum safeguard required to counter the concern of constant surveillance.⁸⁴
71. The applicant submits that the SHD violates the right to an effective judicial remedy, because it allows for no effective *de jure* or *de facto* remedies against violation of the right to the protection of personal data where such data are transferred to the USA. Under the SHD, there is neither a possibility within the EU effectively to challenge violations to the rights to privacy and data protection following the transfer of data to the USA, nor is there one in the US legal system.⁸⁵ There is no point to having high levels of data protection within the EU if data that would be protected within the EU against indiscriminate access and retention may be transferred to a third country that quite plainly does not apply the same standard. Such 'digital refoulement' would, the applicant submits, be the very antithesis of the effective protection of personal data that is guaranteed by the CFR and by the general principles of Union law.
72. The SHD deprives EU citizens and residents, as consumers of companies who transfer their personal data to the US, of an effective right to seek judicial review of the violation of their rights. It manifestly fails to provide, by any benchmark, an adequate standard of protection compared to that which applies within the EU, both under Article 47 CFR and the general principles of Union law, as well as under Directive

Article 6(3) TEU by the Court's consistent case-law: see, e.g.: Case 222/84 *Johnston* [1986] ECR 1651, paras 18 and 19; Case 222/86 *Heylens and Others* [1987] ECR 4097, para 14; Case C-50/00 *Unión de Pequeños Agricultores v Council* [2002] ECR I-6677, para 39; Case C-432/05 *Unibet* [2007] ECR I-2271, para 37; Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakat* [2008] ECR I-6351, para 335; and Joined Cases C-317/08 to C-320/08 *Allassini* [2010] ECR I-2213, para 61.

⁸² The remedy must be available, by analogy to Article 13 ECHR, upon an "arguable claim of violation", and must be effective both in law and in practice: ECtHR Applications Nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 *Silver and Others* §113 ECHR 1975 and Application No 30210/96 *Kudla v Poland* [GC] §157, ECHR 2000-XI.

⁸³ No. 54934/00 of 29 June 2006.

⁸⁴ Para. 37. See also Boehm/de Hert, "Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law", *European Journal of Law and Technology*, Vol. 3, No. 3, 2012.

⁸⁵ TRUSTe, the FTC and US courts lack jurisdiction to find that the SHPs could overrule the FISA. As a non-US person, the applicant also has no right to challenge the FISA. Finally, the DPC refused to investigate the legality of the transfer from the Ireland to the USA.

95/46 and in particular Article 22 thereof, whereunder every person adversely affected by data processing is granted the right to apply for judicial remedies. Instead, under the SHPs (FAQ 11) data subjects are supposed to contact the abovementioned dispute resolution bodies. These bodies are not organised uniformly and establish their own procedural rules. Individuals within the EU can turn to a US-based specialised arbitration entity like TRUSTe or BBBonline to seek clarification whether the company who holds their personal data of EU citizens in the US is violating the terms of the self-certification regime. However, this system of arbitration cannot qualify as an equivalent to an effective judicial review. Private arbitration by bodies such as TRUSTe cannot address violations of the right to the protection of personal data by bodies other than the self-certifying companies. Critically they lack competence to rule on the legality of US governmental agencies' activities. Moreover, such bodies have wide discretion in decision-making and in the selection of remedies but there is no indication within the SHPs that such decisions may then be contested before a court. Thus, data subjects may be cut off from judicial remedies by a decision of such a dispute resolution body.⁸⁶

73. The SHD is thus incompatible with the right to an effective remedy in EU law.
74. This conclusion is reinforced also by the SHPs being based on an approach to dispute settlement which promotes 'unfair' terms under EU consumer protection law contrary to Article 6(1) to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Under Directive 93/13 arbitration clauses putting consumers at a disadvantage in the protection of their rights are not binding on them.⁸⁷ Amongst the indicative list of unfair terms included in the Annex to Directive 93/13 (at paragraph 1(q)) are terms having the object or effect of "*excluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract*". Under the SHPs, consumer complaints fall to be determined by private arbitration bodies. Thus, in the main proceedings, the SHPs are based on the understanding that the applicant, an EU national and resident consumer, is supposed to enter into a contract with Facebook Ireland, an EU registered company, for the provision of social media services to be provided within the EU on his internet-devices, such as his phone and computer that is governed as to the critically important

⁸⁶ Thus, if self-certified 'safe harbor' organisations like Facebook USA fail to comply with the rulings of such bodies, the latter must notify the governmental body with applicable jurisdiction, such as the FTC, who may then seek a court order by filing a complaint in a federal district court. However, it is not obliged to do so and may choose instead to seek an administrative 'cease and desist' order against the organisation. Moreover, the FTC considers itself entitled only to investigate matters falling within s. 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in commerce, a prohibition which would not appear to cover the control of the legality even of "*mass and undifferentiated*" access by US security authorities to the personal data of EU citizens based on US legislation.

⁸⁷ OJ (1993) L 95, p. 29.

issue of the protection of the privacy of his data by the law of a third country, to wit the USA, with which he has no connections. It is difficult to conceive of a more unfair term from a European consumer's perspective.

75. Furthermore, for the consumer Facebook user to 'benefit' from the 'safe harbor' regime with regard to the protection of his personal data, which is transferred to the USA by Facebook Ireland, s/he must agree to settle disputes regarding issues arising with regard to that protection in the USA with a US company (Facebook USA) s/he has no direct contractual relation with, by a US based arbitration company, TRUSTe, which is undertaken in the US and under US law. Thus, practically an entirely EU-focused and located transaction is submitted to the law and the dispute-settlement mechanisms of a third country, in a language (English) which for most EU consumers (including the applicant) is not their mother tongue, and at a place which it would be prohibitively expensive for many to reach. It is, therefore, hardly surprising that the applicant understands that the arbitration mechanisms have in the past 14 years rarely been used by EU nationals affected by data transfers to the US of their personal data. In *Asturcom v Nogueira*,⁸⁸ a case regarding the legality of an arbitration clause in a consumer contract, this Court held that, a national court confronted with such an arbitration clause is "*obliged to assess of its own motion whether that clause is unfair*" in the light of Article 6 of Directive 93/13.⁸⁹ The applicant submits that the SHPs impose grossly unfair terms of contract on consumers with regard to disputes arising from the processing of their personal data. This is incompatible with the requirement to ensure effective judicial protection under Article 47 CFR.

C. Obligation of the DPC to take appropriate action

76. By its second question, the referring court has asked if the DPC "*may and/or must*" conduct its own investigation in the light of the factual developments of EU law. The applicant submits that an answer to this question should be given irrespective of whether the Court invalidates the SHD or interprets the SHD in a way compatible with the fundamental rights under EU law. Member State institutions, bodies and agencies, are obliged when implementing EU law or acting within its scope, to comply in their actions with fundamental rights and other general principles of EU law.⁹⁰ This is also explicitly prescribed in Article 51 CFR.⁹¹ The legality of action of a Member State authority like the DPC is therefore subject not only to national law but also to compliance with general principles of EU law, including the protection of fundamental rights. When the DPC is called upon by a complainant to decide about the legality of the transfer of personal data to third, non-EEA countries, it implements

⁸⁸ Case C-40/08 [2009] ECR I-9579, para. 29.

⁸⁹ See Case C 168/05 *Mostaza Claro* [2006] ECR I-10421, para. 38, and *Asturcom v Nogueira*, loc. cit., paras. 53-54.

⁹⁰ Case C-260/89 *ERT* [1991] ECR I-2925, para 42; Case C-617/10 *Åkerberg* ECLI:EU:C:2013:105, paras 20-27.

⁹¹ As interpreted in, e.g., Case C-617/10 *Åkerberg*, paras 20-27 together with further references.

the provisions of Article 25 and 26 Directive 95/46 under the relevant provisions of the 1998 Irish Act, as amended, that implements the Directive in Ireland. Directive 95/46 is itself, as discussed above, a concretisation of the right to privacy and data protection guaranteed by the general principles of EU law and under Articles 7 and 8 CFR. Given that these provisions correspond to Article 8 ECHR, their meaning and scope, under Article 52(3) CFR, falls to be interpreted in the same way. The ECtHR has held consistently that Article 8 ECHR requires: *"not only that the State refrain from interfering with private life but also entail certain positive obligations on the State to ensure effective enjoyment of this right by those within its jurisdiction."*⁹² It is firmly established that these fundamental rights place a duty on Member States and the Union reasonably to protect them against violations by third parties. Furthermore, Article 47 CFR gives the applicant a right to an effective remedy and a fair trial. Thus, the DPC is obliged to conduct an investigation under the general principles of EU law, since no other possibility exists of investigating whether 'effective enjoyment of' his rights is ensured. In light of the duties of the DPC to protect the fundamental rights of the applicant, he submits that the DPC has an active duty to not only investigate, but, if the complaint is upheld, to use its powers to suspend data flows between Facebook Ireland and Facebook USA in accordance with the law.

IV. CONCLUSION

77. Accordingly, the applicant respectfully proposes to the Court of Justice that it answer the within questions referred to it by the High Court of Ireland as follows:

- 1) A competent national data protection supervisory authority, such as the DPC in the main proceedings, is not bound by the finding of adequacy of protection with regard to US laws and practices contained in Commission Decision 2000/520 by reason of the incompatibility of the latter with Directive 95/46/EC, and Article 25(6) thereof in particular, construed in the light of the requirements of Articles 7, 8 and 47 CFR, as well as Articles 39 TEU and 16 TFEU;
- 2) Articles 7, 8 and 47 CFR, as well as Articles 39 TEU and 16 TFEU, place a positive obligation on national supervisory authorities to ensure effective enjoyment of the rights guaranteed by Directive 95/46, and, consequently, they must investigate arguable complaints made to them regarding infringements of the right to privacy and data protection, such as a complaint regarding mass and undifferentiated access to data transferred to a third country.

Paul O'Shea, Barrister,
Professor Herwig Hofmann, Rechtsanwalt,
Noel J. Travers, Senior Counsel.

⁹² See *Mosley v. United Kingdom*, 10 May 2011, [2011] ECHR 774, with further references.

Original dated this 10th day of November 2014:

Signed: 

Gerard Rudden, Solicitor,
Ahern Rudden Solicitors,
Solicitors for the Applicant,
5 Clare Street,
Dublin 2,
Ireland.

LIST OF ANNEXES

Annex A.1: 'Opinion on the adequacy of the Safe Harbor Decision', Prof. Dr. Franziska Böhm, University of Münster (Germany);

Annex A.2: Complaint by Max Schrems to TRUSTe and response of TRUSTe;

Annex A.3: Complaint by Max Schrems to the US Federal Trade Commission (to date unanswered);

Annex A.4: List of FTC Decisions in the context of 'Safe Harbor Matters' to date (format Excel).